

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY
CAMDEN VICINAGE**

UNITED STATES OF AMERICA

v.

**MOHAMAD IBRAHIM SHNEWER,
DRITAN DUKA,
a/k/a "Distan Duka,"
a/k/a "Anthony Duka,"
a/k/a "Tony Duka,"
ELJvir DUKA,
a/k/a "Elvis Duka,"
a/k/a "Sulayman,"
SHAIN DUKA, and
SERDAR TATAR**

Crim. No. 07-459 (RBK)

SUPPLEMENTAL OPINION

KUGLER, United States District Judge:

Recently before the Court were motions by Defendants Mohamed Ibrahim Shnewer ("Shnewer"), Dritan Duka ("Dritan"), Eljvir Duka ("Eljvir"), Shain Duka ("Shain"), and Serdar Tatar ("Tatar") to suppress evidence obtained pursuant to the Foreign Intelligence Surveillance Act ("FISA"); for disclosure of FISA application papers and orders and for an adversary hearing on their motions to suppress, including a *Franks* hearing; and to declare FISA unconstitutional. This supplemental classified Opinion provides the basis for the Court's denial of Defendants' motions by Order dated August 4, 2008.

[REDACTED]

I. **BACKGROUND**

Defendants are charged with conspiracy to murder members of the U.S. military in violation of 18 U.S.C. § 1117 and attempt to murder members of the U.S. military in violation of 18 U.S.C. §§ 1114 & 2. Shnewer and the three Dukas are also charged with various firearms offenses in violation of 18 U.S.C. §§ 924(c), 922(g)(5), 922(o) & 2 [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

On October 11, 2007, the government filed a notice of intent to introduce at trial evidence obtained pursuant to the Foreign Intelligence Surveillance Act of 1978, as amended, 50 U.S.C. § 1801 *et seq.* (2006). This evidence consists of three things: a December 3, 2006 telephone conversation between Shnewer and Tatar; the week-long audio-video surveillance of Shnewer, the Duka brothers, and others during a February 2007 trip to the Poconos; and an April 12, 2007 telephone conversation between Eljvir Duka and another individual (hereinafter "FISA-obtained evidence"). The government may also offer additional items of FISA-obtained evidence at trial, including in rebuttal. All such items are the fruits of the surveillance or searches authorized by the applications and orders presently at issue and have already been declassified and produced to Defendants.

On June 19, 20 and 23, 2008, Defendants filed their pretrial motions, including

[REDACTED]

motions to suppress some or all of the FISA-obtained evidence.¹ The government filed its opposition to Defendants' motions to suppress the FISA-obtained evidence on July 18, 2008, in both classified and redacted, unclassified forms. Oral argument on these motions was held August 1, 2008.

II. [REDACTED] ANALYSIS

A. [REDACTED] Statutory Overview

[REDACTED] FISA creates a means by which the Executive Branch can gather foreign intelligence information within the United States. "Foreign intelligence information" can signify either (1) "information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against[] (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power," 50 U.S.C. § 1801(e)(1); or (2) "information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to[] (A) the national defense or the security of the United States; or (B) the conduct of the foreign affairs of the United States." 50 U.S.C. §§ 1801(e)(2), 1821(1).

[REDACTED] Under FISA, the government must obtain an order from a judge sitting on the Foreign Intelligence Surveillance Court ("FISA Court") prior to engaging in electronic surveillance or

[REDACTED] The only item of FISA-obtained evidence Tatar asserts standing to challenge is the December 3, 2006 interception of a telephone conversation between Tatar and Shmawar. Tatar was not present during the February 2007 trip to the Poconos nor was he a party to Eljvir's April 12, 2007 conversation.

[REDACTED]

physical searches to collect foreign intelligence information. 50 U.S.C. §§ 1804(a), 1805(f), 1823(a), 1824(e). To do so, the government files with the FISA Court an ex parte, under seal application, approved by the Attorney General. See 50 U.S.C. §§ 1804(a), 1823(a). If the government's application meets the statutory requirements, then the reviewing judge on the FISA Court must issue an order. 50 U.S.C. §§ 1805(a), 1824(a). Electronic surveillance or physical searches may be approved for up to 90 days for a "United States person,"² or up to 120 days for a non-"United States person."³ 50 U.S.C. §§ 1805(e), 1824(d). The FISA Court may grant extensions of orders "upon an application . . . and new findings made in the same manner as required for an original order." 50 U.S.C. §§ 1805(e)(2), 1824(d)(2).

[REDACTED] If the government intends to use or disclose at a criminal trial evidence collected pursuant to a FISA Court order, the government must first notify the defendant and the district court. 50 U.S.C. §§ 1806(c), 1825(d). An "aggrieved person"⁴ has two grounds for seeking suppression: he can assert the evidence was unlawfully acquired and he can assert the electronic surveillance or physical search was not carried out in compliance with the FISA Court's order.

² [REDACTED] FISA defines "United States person" to include citizens of the United States and aliens lawfully admitted for permanent residence. 50 U.S.C. § 1801(i).

³ [REDACTED] FISA actually states orders may be valid for these specified time periods or "for the period necessary to achieve its purpose," 50 U.S.C. § 1805(e)(1); however, courts routinely ignore that alternative, presumably because the FISA Court adheres to the 90 and 120 day restrictions.

⁴ [REDACTED] FISA defines an "aggrieved person" with respect to electronic surveillance as "a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance." 50 U.S.C. § 1801(k). With regard to physical searches, FISA defines an "aggrieved person" as a "person whose premises, property, information, or material is the target of physical search or any other person whose premises, property, information, or material was subject to physical search." 50 U.S.C. § 1821(2).

[REDACTED]

[REDACTED]

50 U.S.C. §§ 1806(e), 1825(f). In response, the Attorney General can file an affidavit certifying that "disclosure or an adversary hearing would harm the national security of the United States," thereby invoking a privilege. 50 U.S.C. §§ 1806(f), 1825(g). In that case, FISA requires the court to conduct an in camera, ex parte review of the challenged application, order, and other such materials relating to the surveillance to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. *Id.*

[REDACTED] To decide a motion to suppress, the court must in camera, ex parte review the following findings made by the FISA Court in authorizing the surveillance and searches:

(1) the President has authorized the Attorney General to approve applications for electronic surveillance [or physical searches] for foreign intelligence information;

(2) the application has been made by a Federal officer and approved by the Attorney General;

(3) on the basis of the facts submitted by the applicant there is probable cause to believe that—

(A) the target of the electronic surveillance [or physical search] is a foreign power or an agent of a foreign power. Provided, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States; and

(B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power [or the premises or property to be searched is owned, used, possessed by, or is in transit to or from an agent of a foreign power or a foreign power];

(4) the proposed minimization procedures meet the definition of minimization procedures under section 1801(h) of this title; and

(5) the application which has been filed contains all statements and certifications required by section 1804 of this title and, if the target is a United States person, the certification or certifications are not clearly erroneous on the basis of the

[REDACTED]

statement made under section 1804(a)(7)(E) of this title and any other information furnished under section 1804(d) of this title.

50 U.S.C. § 1805(a) (regarding electronic surveillance); see also 50 U.S.C. § 1824(a) (concerning physical searches).

[REDACTED] FISA defines a "foreign power" as: (1) a foreign government or any component thereof, whether or not recognized by the United States; (2) a faction of a foreign nation or nations, not substantially composed of United States persons; (3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments; (4) a group engaged in international terrorism or activities in preparation therefor; (5) a foreign-based political organization, not substantially composed of United States persons; or (6) an entity that is directed and controlled by a foreign government or governments. 50 U.S.C. § 1801(a).

[REDACTED] An "agent of a foreign power" is:

(1) any person other than a United States person, who--

(A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power . . . ;

(B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or

(C) engages in international terrorism or activities in preparation therefore;
or

(2) any person who--

(A) knowingly engages in clandestine intelligence gathering activities for

[REDACTED]

or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;

(B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;

(C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power;

(D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or

(E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).

50 U.S.C. § 1801(b).

[REDACTED] If during the court's review, the judge decides he cannot make an accurate determination of the legality of the surveillance in camera and ex parte, he "may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance." 50 U.S.C. §§ 1806(f).³ If the judge decides any of the surveillance or search was unlawfully authorized or conducted, FISA calls for suppression of all fruits of that surveillance or search. 50 U.S.C. §§

³ [REDACTED] The language with respect to physical searches differs slightly: "the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the physical search, or may require the Attorney General to provide to the aggrieved person a summary of such materials, only where such disclosure is necessary to make an accurate determination of the legality of the physical search." 50 U.S.C. § 1825(g).

[REDACTED]

1806(g), 1825(h). If the surveillance or search is deemed to have been lawful, however, the motion to suppress must be denied, "except to the extent that due process requires discovery or disclosure." 50 U.S.C. §§ 1806(g), 1825(h).

B. [REDACTED] Motions to Compel Disclosure

[REDACTED] Each Defendant moves the Court to compel disclosure of the government's FISA applications, warrants, orders, and other supporting materials. Defendants assert four arguments in support of their motion to compel. First, they argue the adversary process is necessary for the court to make an accurate assessment of the legality of the surveillance. They argue further that there is no evidence they were agents of a foreign power. In addition, they maintain there is no basis for a good faith showing of risk of harm to national security warranting nondisclosure, considering all fruits of the surveillance that has been declassified, the identities of two cooperating witnesses are known, and the investigation into Defendants has ended. Finally, Defendants argue they should be given access to the FISA application materials because their attorneys each have security clearance.

[REDACTED] The government opposes any such disclosure, arguing the Court is equipped to make an accurate determination of the legality of the collection without disclosing the FISA application materials. To this end, the government submitted a classified filing to facilitate the Court's in camera, ex parte review. In responding to Defendants' arguments, the government asserts an in camera, ex parte review reflects Congress's considered judgment in balancing national security interests with civil liberties, and Defendants have offered no sound basis for rejecting that judgment. Moreover, the government argues the Court is capable of reviewing the FISA Court's probable cause determination and certification requirements without the aid of defense counsel.

[REDACTED]

The government submits there is a good faith basis for the Attorney General to assert the risk of harm to national security warranting nondisclosure and that security clearance does not automatically entitle defense counsel to review classified materials in this case.

[REDACTED] In response to Defendants' argument that the Court should be skeptical of the Attorney General's declaration and claim of privilege, the government argues that just because [REDACTED] FISA-obtained evidence has been declassified does not mean materials submitted to the FISA Court should be. The government argues further that [REDACTED]

[REDACTED] there are [REDACTED] sources whose disclosure would harm national security, and disclosure of the materials submitted to the FISA Court could jeopardize ongoing investigations or national security interests.

[REDACTED] Ex parte and in camera inspections are the rule under FISA. United States v. Abu-Jihaad, 531 F. Supp. 2d 299, 310 (D. Conn. 2008). In fact, it appears that no district or appellate court has ever deemed disclosure necessary. Courts have only addressed instances where disclosure would be necessary in the hypothetical, anticipating it would be appropriate where a district court's "initial review of the application, order, and fruits of the surveillance indicates that the question of legality may be complicated by factors such as 'indications of possible misrepresentation of fact, vague identification of the persons to be surveilled, or surveillance records which include a significant amount of nonforeign intelligence information, calling into question compliance with the minimization standards contained in the order.'" See, e.g., United States v. Belfield, 692 F.2d 141, 147 (D.C. Cir. 1982) (quoting S. Rep. No. 95-701, 95th Cong., 2d Sess. 64 (1978)).

[REDACTED] In this case disclosure is not necessary. The government has submitted the [REDACTED] FISA

[REDACTED]

dockets [REDACTED] complete with declarations, certifications, orders, and other related materials. The government has also provided the FISA Court dockets regarding [REDACTED] whose communications [REDACTED] undergird in part the probable cause determination at issue to this case. In addition, the government has included the classified declaration [REDACTED] detailing how investigators effectuated appropriate minimization; the Attorney General's unclassified declaration and claim of privilege; the classified declaration of FBI Deputy Assistant Director [REDACTED] supporting the Attorney General's claim of privilege; and the FBI's standard minimization procedures and standard techniques for electronic surveillance and searches. These materials are well organized and readily understandable. Therefore, it is not necessary to disclose any portion of them to Defendants to determine whether the electronic surveillance and searches in this case were lawfully authorized and conducted.

C. [REDACTED] Motions to Suppress for Failure to Satisfy FISA's Statutory Requirements

[REDACTED] In the event the Court denies Defendants' motion to compel disclosure, Defendants ask the Court to suppress the fruits of the FISA surveillance based on the Court's own determination that the surveillance and searches were unlawfully authorized and conducted. In particular, Defendants argue the applications to the FISA Court did not support the finding of probable cause. They also contend the certifications by the executive branch official were inadequate. Lastly, they submit the government failed to comply with FISA's minimization requirements in carrying out the orders. The Court will address each of these grounds for suppression in turn.

[REDACTED]

Defendants assert they are not "a foreign power" or "agent[s] of a foreign power." Based on the government's perceived concession of that point, Defendants posit that the application papers the government submitted to the FISA Court could not have demonstrated probable cause to believe otherwise.⁶ In addition, Defendants suggest that the FISA Court application papers fail to demonstrate probable cause to believe the telephones subjected to electronic surveillance and the physical facilities that were bugged were being used or were about to be used by a foreign power or an agent of a foreign power. Defendants argue further that even if the government had facts supporting FISA's probable cause requirement at the beginning of its investigation of Defendants, the government could not possibly have still had the necessary probable cause more than a year later, because they obtained no foreign intelligence information during their surveillance.

The government counters that the applications to the FISA Court contain a sufficient basis for a determination of probable cause [REDACTED] Initially, the government argues the FISA Court correctly identified al Qaeda as a foreign power, as defined in 50 U.S.C. § 1801(s)(4), because it qualifies as "a group engaged in international terrorism or activities in preparation therefor." In addition, the government argues the FISA

Tatar explores this contention the most thoroughly, relying on the information contained in the warrant application used in connection with the search of his apartment, the Complaint, and other unclassified or declassified material to guess at the government's possible basis for suspecting him of being an agent of a foreign power. He cites the sole references to foreign powers in the totality of the known evidence: Shrewer telling CW-1 that the group of them wanted CW-1 to help lead the attack based on his experience in the Egyptian military; Eljvir Duka's suggestion that the group needed to receive a fatwa before they could attack; and Dritan Duka's statement that AK-47s are easier to purchase overseas, particularly in Lebanon. Tatar maintains none of this evidence suffices as a foundation for probable cause to believe he was an agent of a foreign power.

[REDACTED]

Court appropriately found probable cause to believe [REDACTED] were agents of al Qaeda, as defined in section 1801(b)(2)(E), because each knowingly engaged, or knowingly aided, abetted, or conspired with any other person, in international terrorism, or activities in preparation therefore, for or on behalf of a foreign power.

[REDACTED] As an initial matter, the Court must address the standard of review with respect to the FISA Court's probable cause determinations. Despite the government's contention otherwise, the appropriate standard of review for this Court's in camera, ex parte review is de novo. The government maintains this Court should accord deference to the FISA Court's probable cause determination, citing United States v. Pelton, 835 F.2d 1067 (4th Cir. 1987), and United States v. Badia, 827 F.2d 1458 (11th Cir. 1987). These cases are not persuasive on this point, however. The deferential standard of review employed in Pelton, 835 F.2d at 1076—" [w]here, as here, the statutory application was properly made and earlier approved by a FISA judge, it carries a strong presumption of veracity and regularity in a reviewing court"—has since been rejected by the Fourth Circuit. See United States v. Hammoud, 381 F.3d 316, 332 (4th Cir. 2004) (conducting de novo review), vacated on other grounds, 543 U.S. 1097 (2005); United States v. Squillacote, 221 F.3d 542, 554 (4th Cir. 2000) (same). Moreover, Badia does not speak of deference, but states only, "in determining the legality of a surveillance . . . the trial judge . . . [is] not to make determinations which the issuing judge is not authorized to make." Badia, 827 F.2d at 1463 (quoting H.R. Rep. 1283, pt. I, 95th Cong., 2d Sess. 25 (1978)). In recent years, district courts have uniformly employed de novo review with no deference accorded to the FISC's probable cause determinations. See United States v. Wagsama, 547 F. Supp. 2d 982, 990 (D. Minn. 2008) ("Because the FISA review is ex parte, the Court rejects the prosecution's contention that the

[REDACTED]

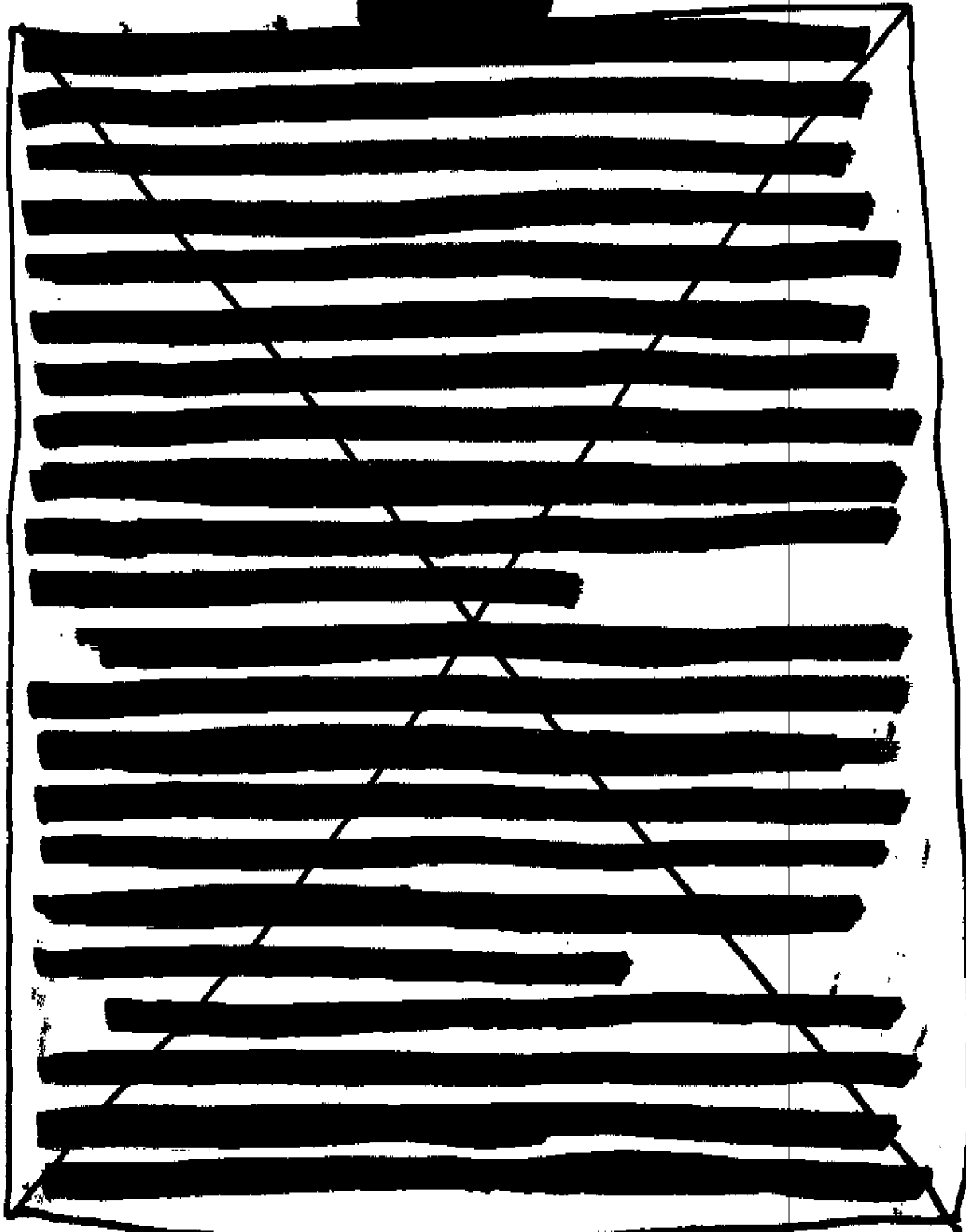
FISC's probable cause determinations are entitled to "substantial deference."); United States v. Mubayyid, 521 F. Supp. 2d 125, 131 (D. Mass. 2007) ("In essence, this Court is required to conduct the same review of the FISA materials that the FISC itself conducted."); United States v. Rosen, 447 F. Supp. 2d 538, 545 (E.D. Va. 2006) (rejecting government's argument that review entails deference to FISA Court's probable cause determination).

[REDACTED] "[P]robable cause is a fluid concept—turning on the assessment of probabilities in particular factual contexts." Illinois v. Gates, 462 U.S. 213, 232 (1983). While probable cause requires more than mere suspicion, it does not require evidence sufficient to prove facts beyond a reasonable doubt. Orsatti v. N.J. State Police, 71 F.3d 480, 482-83 (3d Cir. 1995). The Third Circuit instructs that courts should apply a "common sense approach," based on the totality of the circumstances, to determine whether probable cause existed. Paff v. Kaltenbach, 204 F.3d 425, 436 (3d Cir. 2000). Moreover, in making probable cause determinations under FISA, a reviewing judge may "consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target." 50 U.S.C. §§ 1805(b), 1824(b).

I. [REDACTED] Whether each target was an agent of a foreign power

[REDACTED] The Court concludes each of the applications to the FISA Court contained sufficient support for the finding of probable cause to believe [REDACTED] were agents of a foreign power, namely al Qaeda. Al Qaeda is a foreign power as FISA defines that term. See 50 U.S.C. § 1801(a) (including in definition "a group engaged in international terrorism or activities in preparation therefor"). Indeed, several courts have found as much. See, e.g., Warane, 547 F. Supp. 2d at 991; United States v. Bin Laden, 126 F. Supp. 2d 264, 278 (S.D.N.Y. 2000). Next, the Court will detail its review of whether the application materials support probable cause to

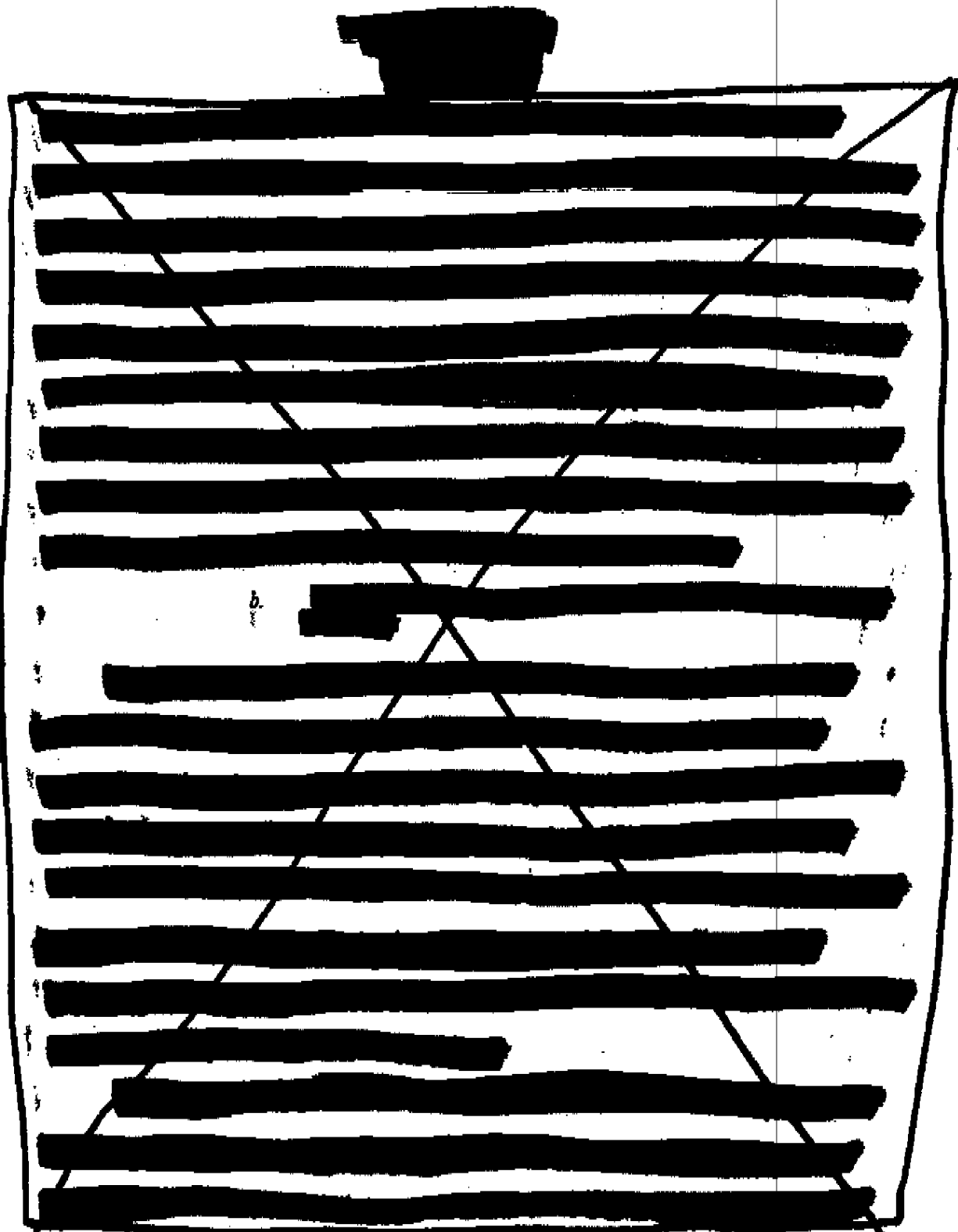
believe [REDACTED] were agents of al Qaeda.

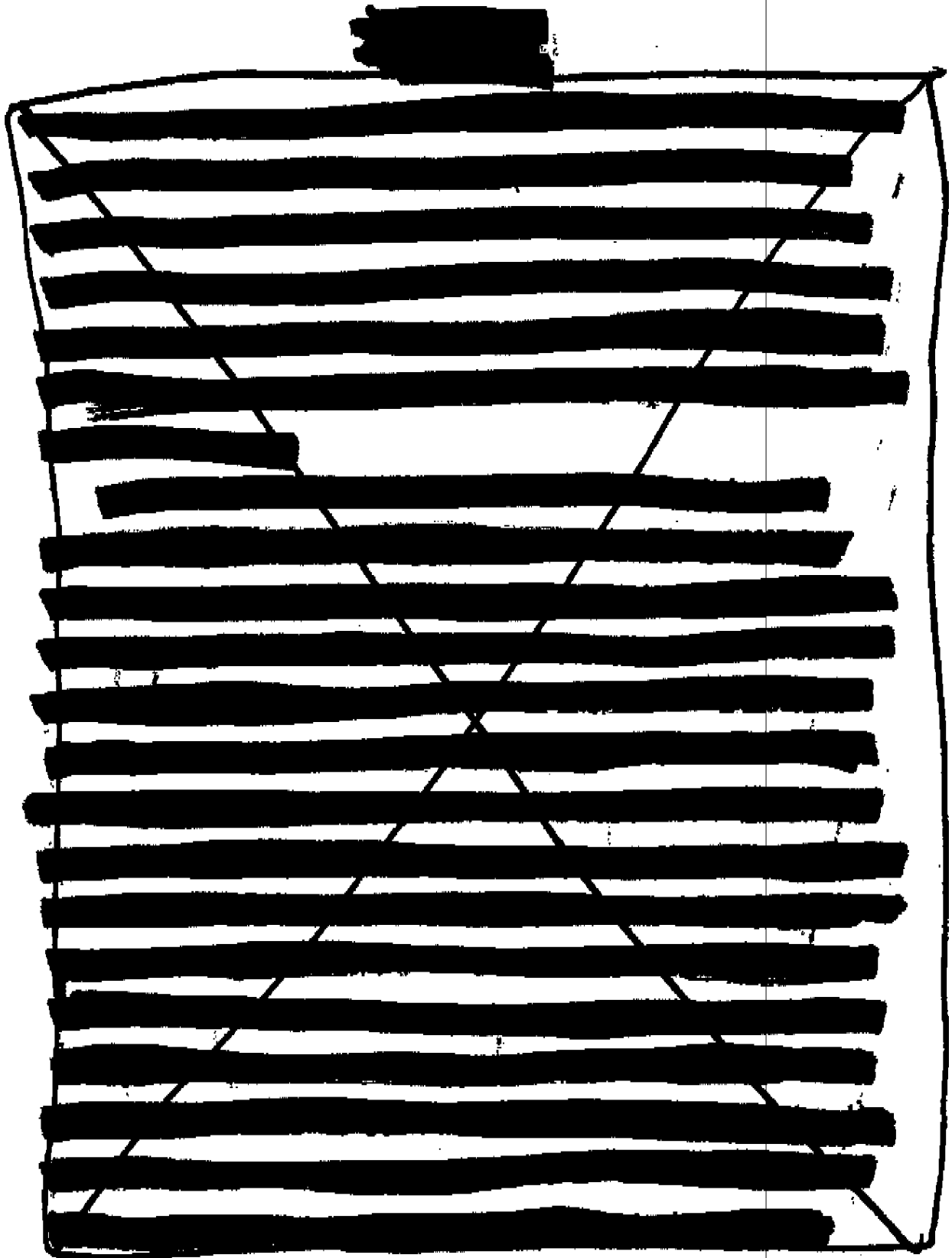


[REDACTED]

Considering the totality of the circumstances, the FISA Court's probable cause determination [REDACTED] was well-founded. [REDACTED]

[REDACTED]





[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Consequently, [REDACTED]

[REDACTED] this Court concurs with the FISA Court's probable cause determination that [REDACTED] was an agent of al Qaeda.

[REDACTED]

This application [REDACTED] sets forth probable cause to believe [REDACTED] was an agent of al Qaeda. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

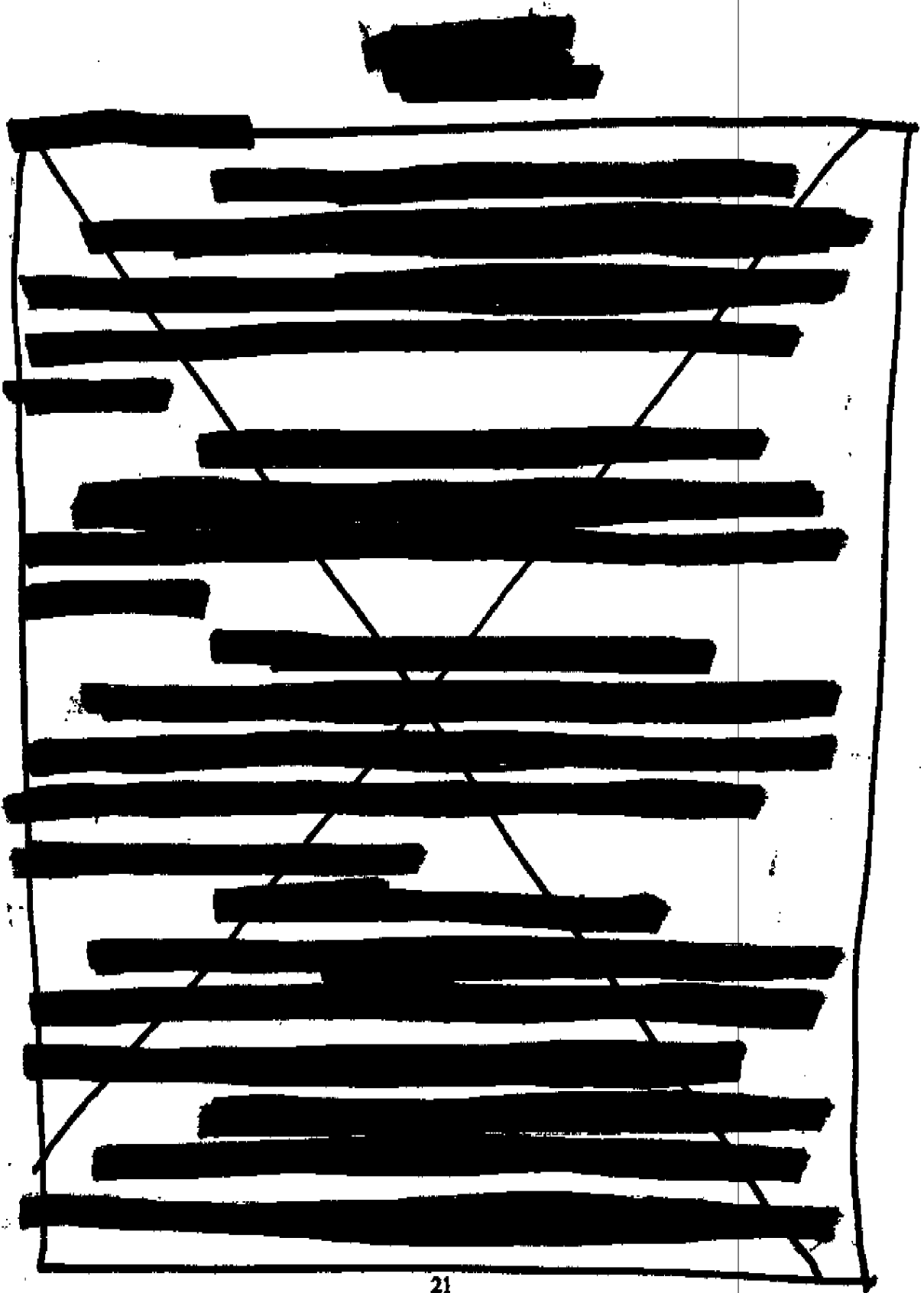
[REDACTED]

[REDACTED]

- ii. Whether the facilities at which the electronic surveillance would be directed were being used or were about to be used by the target or whether the premises or properties to be searched contained foreign intelligence information and were owned, used, possessed by, or in transit to or from the target

The probable cause determinations regarding the facilities to be surveilled and properties or premises to be searched follow from the probable cause determination that [REDACTED]

[REDACTED] were agents of al Qaeda. [REDACTED]



[illegible]

iii. Whether for any U.S.-person target, the finding of probable cause was not based solely on First Amendment-protected activities

[REDACTED]

[REDACTED]

[REDACTED] This requirement, [REDACTED] was met in this case. "[N]o United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States." 50 U.S.C. § 1805(a)(3)(A). Where "speech is the instrumentality of the crime itself, the First Amendment provides no shelter from the government's exercise of its otherwise valid police powers." United States v. Dwinells, 508 F.3d 63, 71 (1st Cir. 2007). [REDACTED]

[REDACTED]

[REDACTED] This speech therefore is an instrumentality of a crime and is not protected by the First Amendment. Accordingly, [REDACTED] was not a target of FISA surveillance and searches based exclusively on protected speech.

B. [REDACTED] Sufficiency of Executive Branch Official's Certifications

[REDACTED] As a second basis for suppression of the FISA-obtained evidence, Shnewer, Eljvir, and Dritan (joined by Tatar and Shain) assert that two of the certification requirements were either absent or inadequate. They challenge the presence or adequacy of the certifications that the certifying official deems the information sought to be foreign intelligence information and that a significant purpose of the surveillance is to obtain foreign intelligence information. Shnewer, an American citizen, asserts specifically that the certifications submitted with the FISA application papers were clearly erroneous as to these assertions.

[REDACTED] In addition, Tatar argues the investigation into the defendants became a criminal investigation rather than a matter of foreign intelligence gathering at least by December 3, 2006, the date Tatar's conversation with Shnewer was intercepted. The government counters, "a certification that a 'significant purpose' of the surveillance is to collect foreign intelligence

[REDACTED]

information is not clearly erroneous merely because the Government was concurrently engaging in a criminal and a foreign intelligence investigation of a target or could anticipate that the fruits of the FISA collection may later be used, as allowed by Section 1806(b), as evidence in a criminal trial." Lastly, there are several other certification requirements that must be met before a FISA order is issued, which are detailed below. Although Defendants have not specifically challenged the others, this Court must still satisfy itself during its in camera review that they were present and where necessary, not clearly erroneous. The government maintains that all certification requirements were fulfilled and that these certifications were not inconsistent with the criminal investigation that grew out of the FISA-approved surveillance.

[REDACTED] included in the requirements for an application to the FISA Court, an authorized executive branch official must certify the following: (1) that the certifying official deems the information sought to be foreign intelligence information; (2) that a significant purpose of the surveillance is to obtain foreign intelligence information; (3) that the information cannot reasonably be obtained by normal investigative techniques. §§ 1804(a)(7)(A)-(C).

1823(a)(7)(A)-(C). The application must also designate the type of foreign intelligence information being sought according to the categories described in section 1801(e) and include a statement of the basis for the certification that (i) the information sought is the type of foreign intelligence information designated, and (ii) such information cannot reasonably be obtained by normal investigative techniques. §§ 1804(a)(7)(D)-(E), 1823(a)(7)(D)-(E).

[REDACTED] Certifications submitted in support of a FISA application are entitled to a presumption of validity. United States v. Duggan, 743 F.2d 59, 77 n.6 (2d Cir. 1984) (citing Evans v. Delaware, 438 U.S. 154 (1978)). For U.S. persons challenging a certification, the

[REDACTED]

reviewing court must determine whether it appears from the application as a whole that the certification is not clearly erroneous. United States v. Rahman, 861 F. Supp. 247, 251 (S.D.N.Y. 1994) (citing 50 U.S.C. §§ 1805(a)(5) and 1824(a)(5)); see also In re Sealed Case, 310 F.3d 717, 739 (F.I.S.C. Rev. 2002) ("When the target is a U.S. person, the FISA judge reviews the certification for clear error."). "A finding is 'clearly erroneous' when although there is evidence to support it, the reviewing court on the entire evidence is left with the definite and firm conviction that a mistake has been committed." United States v. U.S. Gypsum Co., 333 U.S. 364, 395 (1948).

FISA does not specify a standard of review for certifications concerning non-U.S. persons. The government takes this to mean the reviewing court need only determine the requisite certifications were present; however, Congress arguably intended that a non-U.S. person could prevail on "a prima facie showing of a fraudulent statement by a certifying officer." H.R. Rep. 1283, pt. I, 95th Cong., 2d Sess. 25 (1978) (noting further, "procedural regularity is the only determination to be made if a non-U.S. person is the target").

[REDACTED]

[REDACTED]

[illegible]

[REDACTED]

[REDACTED]

[REDACTED]

C. [REDACTED] Minimization

[REDACTED] Defendants argue the government failed to follow FISA's minimization procedures. They base this argument on the large volume of FISA-obtained discovery that seemingly bears no relationship to either criminal activity or national security. The government advances three arguments in support of their compliance with FISA's minimization requirements. First, [REDACTED] they cannot tell based on the discovery what the government in fact minimized and what it did not. In addition, the question for the Court "is not whether the defense can come up with an innocent explanation for a particular recording, but whether, at the time of minimization, it was reasonably evaluated as containing foreign intelligence information or not." Lastly, the government argues it is not a violation of FISA's minimization requirements to [REDACTED] particularly under the circumstances present in this case.

[REDACTED] Each application to the FISA Court must contain a "statement of the proposed minimization procedures." 50 U.S.C. §§ 1804(a)(5), 1823(a)(5). Included among the prerequisites for issuing an order, the FISA judge must determine that the proposed minimization procedures comply with the statutory definition of minimization procedures. See 50 U.S.C. §§ 1805(a)(4), 1824(a)(4). FISA defines minimization procedures to mean, in pertinent part:

- (1) specific procedures adopted by the Attorney General that are reasonably designed in light of the purpose and technique of the particular surveillance or search, to minimize the acquisition and retention, and prohibit the dissemination,

[REDACTED]

of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;

(2) procedures that require that nonpublicly available information, which is not foreign intelligence information, shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance;

(3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes.

See 50 U.S.C. §§ 1801(h)(1), 1821(4).

[REDACTED] The reasonableness of the minimization practices should be evaluated based on the facts and circumstances of each case. In *re Scaled Case*, 310 F.3d at 740. "Less minimization in the acquisition stage may well be justified to the extent the intercepted communications are 'ambiguous in nature or apparently involve[] guarded or coded language,' or 'the investigation is focusing on what is thought to be a widespread conspiracy [where] more extensive surveillance may be justified in an attempt to determine the precise scope of the enterprise.'" *Id.* at 741 (citing *Scott v. United States*, 436 U.S. 128, 140 (1978)); see also *Hammond*, 381 F.3d at 334 ("The minimization requirement obligates the Government to make a good faith effort to minimize the acquisition and retention of irrelevant information."); *Rosen*, 447 F. Supp. 2d at 551 ("Acknowledging the inherent difficulty in determining whether something is related to clandestine activity, courts have construed 'foreign intelligence information' broadly and sensibly allowed the government some latitude in its determination of what is foreign intelligence information."). In addition, less minimization at acquisition is reasonable where the targets of

FISA surveillance speak a foreign language for which there is no contemporaneously available translator. See In re Sealed Case, 310 F.3d at 741.

According to the FISA Court of Review, the normal practice in carrying out electronic surveillance pursuant to a FISA order is to leave the surveillance devices on continuously, "and the minimization occurs in the process of indexing and logging the pertinent communications." Id. at 740. Courts have apparently found this practice reasonable. See, e.g., Hammond, 381 F.3d at 334 ("the mere fact that innocent conversations were recorded, without more, does not establish that the government failed to appropriately minimize surveillance."); Rosen, 447 F. Supp. 2d at 552 (excusing any failures by government to properly minimize electronic surveillance as inadvertent, disclosed the FISA Court on discovery, or promptly rectified); Rahman, 861 F. Supp. at 252-53 (finding minimization requirements fulfilled where government apparently recorded all calls rather than monitoring intermittently and captured conversations to which no targeted person was a party).

In this case, the proposed minimization procedures contained in the materials presented to the FISA Court satisfy the statutory requirements. In the classified declaration of [REDACTED] he reveals that in carrying out the FISA orders at issue in this case investigators employed the FBI's standard minimization procedures, adopted by the U.S. Attorney General and filed with the FISA Court. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Applying these procedures, the vast majority of the collection was deemed nonpertinent and therefore minimized. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] The Court agrees that [REDACTED] was reasonable in this case, and because the standard minimization procedures used here have continually met with the approval of reviewing courts, this Court finds that the FBI complied with FISA's minimization requirements. Defendants' motion to suppress on this ground is denied.

D. [REDACTED] Content of Order

[REDACTED] Although not challenged by Defendants, during its ex parte, in camera review this Court also ensured that the FISA orders in this case demonstrated the required specificity. FISA requires the FISA Court's order authorizing surveillance or searches to specify: (1) the identity (or a description of) the specific target of the collection; (2) the nature and location of each

[REDACTED]

[REDACTED]

[REDACTED]

facility or place at which the electronic surveillance will be directed or of each of the premises or property to be searched; (3) the type of information sought to be acquired and the type of communications or activities to be subjected to the electronic surveillance, or the type of information, material, or property to be seized, altered, or reproduced through the physical search; (4) the means by which electronic surveillance will be effected and whether physical entry will be used to effect the surveillance, or a statement of the manner in which the physical search will be conducted; (5) the period of time during which the electronic surveillance or physical search is approved; and (6) the applicable minimization procedures. 50 U.S.C. §§ 1805(c)(1)(A)-(F), 1824(c)(1)(A)-(E). The Court's finds that each order issued by the FISA Court related to this case contained all the necessary information.

III. [REDACTED] FRANKS CHALLENGE

[REDACTED] In addition to moving for disclosure of the FISA applications and related materials under the provisions for such disclosure in FISA, Shnewer also asks for a Franks hearing. Shnewer bases this motion on his contention that the FISA Court application papers contain false statements, recklessly made, in violation of Franks v. Delaware, 438 U.S. 154 (1978). The government responds that Defendants are not entitled to a Franks hearing because they have offered no facts in support of their assertion regarding reckless falsehoods. Furthermore, the government asserts there is no basis for finding any FISA application contained a reckless and material false statement or omission.

[REDACTED] Despite noting a small number of inaccuracies or inconsistencies in the FISA applications, the government asserts those deficiencies do not alone or together make a material difference to the FISA Court's probable cause findings. [REDACTED]

[REDACTED]

[REDACTED] Moreover, the government argues there is no basis for believing these misstatements were intentionally or recklessly made.

[REDACTED] Challenges to the validity of a warrant based on allegations that the accompanying affidavit contains material false statements are governed by Franks. Where a warrant has issued, the supporting affidavit is entitled to a presumption of validity. Id. at 171. The party disputing the veracity of the warrant application can challenge the validity of the warrant only by making a substantial preliminary showing that the affiant deliberately or recklessly included falsehoods in or omitted information from the underlying affidavit concerning material facts necessary to the determination of probable cause. Id. at 155-56; United States v. Calisto, 838 F.2d 711, 714-16 (3d Cir. 1988) (expanding Franks analysis to omissions). A substantial preliminary showing requires "an offer of proof." United States v. Chandia, 514 F.3d 365, 373 (3d Cir. 2008). If the defendant establishes falsity or material omission by a preponderance of the evidence, the false statements will be stricken from the affidavit and the court will determine whether the information remaining in the affidavit is sufficient to support a finding of probable cause. Franks, 438 U.S. at 155-56.

[REDACTED] There is no binding authority establishing that Franks applies in the context of FISA; however, several courts have conducted Franks analyses in FISA cases either affirmatively or *arguendo*. For example, the Second Circuit found that a defendant could be entitled to a Franks hearing in connection with FISA surveillance. Duggan, 743 F.2d at 77 n.6; see also United States v. Dammah, 412 F.3d 618, 624-25 (6th Cir. 2005) (assuming *arguendo* Franks applies to FISA proceedings); Mubavvi, 521 F. Supp. 2d at 130 (assuming Franks or equivalent principles inhere in FISA cases).


[REDACTED]


[REDACTED] There is insufficient basis for a Franks hearing in this case. Because there has been no disclosure of the materials underlying the FISA warrants in this case, it is seemingly impossible for Defendants to make the necessary "substantial showing" of a reckless or intentional falsehood or omission "accompanied by and offer of proof." This catch-22 has not troubled courts, however, and they defer to FISA's statutory scheme. See, e.g., Mubayyid, 521 F. Supp. 2d at 131 ("The balance struck under FISA—which is intended to permit the gathering of foreign intelligence under conditions of strict secrecy, while providing for judicial review and other appropriate safeguards—would be substantially undermined if criminal defendants were granted a right of disclosure simply to ensure against the possibility of a Franks violation."); see also Abu-Jibane, 531 F. Supp. 2d at 311-12 (rejecting Franks challenge); United States v. Hassoun, 2007 WL 1068127, at *4 (S.D. Fla. Apr. 4, 2007) (finding Franks challenge lacked merit where no offer of proof and substantial grounds for not revealing classified materials); [REDACTED]

[REDACTED] None of the inaccuracies highlighted by the government appear to have been made intentionally or recklessly. See Franks, 438 U.S. at 171 (finding allegations of negligence or innocent mistake are insufficient, as are allegations of immaterial misrepresentations or omissions). Furthermore, even if the Court were to determine there existed a reckless or intentional falsehood or omission in the FISA application materials, the evidence obtained still should not be suppressed unless the Court makes the further finding that the falsehood or omission was material to the probable cause determination. Here, none of the inaccuracies jeopardize the probable cause findings.



IV. CONSTITUTIONALITY OF FISA

 Defendants Shnewer and Tatar explicitly challenge the constitutionality of the FISA, and the other Defendants join in these arguments as well. Eljvir additionally argues turning the investigation over to domestic criminal prosecution rendered the surveillance of him improper and violated his Fourth Amendment rights. Defendants focus their arguments on the "significant purpose" test and argue that this standard contravenes the Fourth Amendment. The government argues that FISA is constitutional because the collection it authorizes is reasonable under the Fourth Amendment.

 FISA followed the decision of the United States Supreme Court in United States v. United States District Court for the Eastern District of Michigan, 407 U.S. 297 (1972) ("Keith"), where the Court, while not commenting on the power of the executive in the context of surveillance of foreign powers, held that electronic surveillance in domestic security matters requires prior judicial approval. Keith, 407 U.S. at 323. FISA, as initially passed by Congress, required that a FISA application include a certification that the "primary purpose" of the surveillance be to gather foreign intelligence information. In re Sealed Case, 310 F.3d 717, 722 (For. Intell. Surv. Rev. 2002). Whether intended by Congress or not, the result of the "primary purpose" test was the creation of a belief that it was inappropriate to use FISA-derived evidence in criminal prosecution. In re Sealed Case, 310 F.3d at 723, 727-28. Thus, a "wall" was created between the intelligence officials conducting foreign intelligence investigations and those preparing for criminal prosecutions. In 2001, the USA Patriot Act, Pub. L. 107-56, § 218 (2001), amended FISA at section 1804(a)(6)(B) so that foreign intelligence goals no longer had to be the primary purpose of the surveillance but instead merely a "significant purpose." In re Sealed

[REDACTED]

Case 310 F.3d at 728-29.

[REDACTED] Before the Patriot Act amendments, it appears that every court with the occasion to consider FISA's constitutionality determined FISA was constitutional. See, e.g., In re Grand Jury Proceeding, 347 F.3d 197, 206 (7th Cir. 2003). After the Patriot Act was passed, the FISA Court of Review ("Court of Review") was convened for the first and only time to consider the "significant purpose" test and its consistency with the Fourth Amendment. In re Sealed Case, 310 F.3d 717 (For. Intell. Surv. Rev. 2002). The groups challenging the constitutionality of FISA in that case argued that any government surveillance whose primary purpose is criminal prosecution of whatever kind is per se unreasonable if not based on a warrant. Id. at 737.

[REDACTED] The Court of Review discussed the differences between a Title III warrant and a FISA order and noted that "to the extent a FISA order comes close to meeting Title III, that certainly bears on its reasonableness under the Fourth Amendment." Id. at 742. The Court of Review concluded that "while Title III contains some protections that are not in FISA, in many significant respects the two statutes are equivalent, and in some, FISA contains additional protections." Id. at 741. The Court of Review also analyzed the Supreme Court's "special needs" cases, noting that the government can sometimes conduct warrantless and suspicionless searches when special needs, beyond the normal need for law enforcement, call for them. The Court of Review concluded that "FISA's general programmatic purpose, to protect the nation against terrorists and espionage threats directed by foreign powers, has from its onset" been different from ordinary law enforcement. Id. at 746. Though noting the lack of a definite jurisprudential answer regarding consistency with the Fourth Amendment, the Court decided that it "believe[d] firmly" that FISA, as amended by the Patriot Act, is constitutional "because the

[REDACTED]

surveillances it authorizes are reasonable." Id. at 746.

[REDACTED] Of the courts asked to rule on the constitutionality of FISA since In re Sealed Case, most have adopted its conclusions. See, e.g., Mubayyid, 521 F. Supp. 2d at 139-40 (holding that FISA does not violate the probable cause requirement of the Fourth Amendment though the probable cause determination uses a lesser standard and explicitly agreeing with In re Sealed Case that the significant purpose test is constitutional); Abu-Jihaad, 531 F. Supp. 2d at 305-09 (noting pre-Patriot Act Second Circuit rule in upholding the constitutionality of FISA, agreeing with In re Sealed Case, and concluding that the FISA as amended is constitutional).

[REDACTED] Only one court has yet found FISA is unconstitutional. See Mayfield v. United States, 504 F. Supp. 2d 1023 (D. Or. 2007). The Mayfield court explicitly rejected the reasoning of In re Sealed Case with regard to the significant purpose test, believing that the Court of Review ignored "congressional concern between intelligence gathering and criminal law enforcement." Id. at 1041-42. The Mayfield court cited separation of powers issues and a worry that "the constitutionally required interplay between Executive action, Judicial decision, and Congressional enactment" was eliminated by the Patriot Act amendments. The court held FISA as amended by the Patriot Act to be unconstitutional because surveillance pursuant to a FISA warrant could "have as its 'programmatic' purpose the generation of evidence for law enforcement purposes—which is forbidden without criminal probable cause and a warrant." Id. at 1042.

[REDACTED] Although Mayfield is the only case to find the FISA unconstitutional, one other court has expressed doubts about FISA's consistency with the Fourth Amendment while upholding the FISA-obtained materials at issue in that case. See Warsame, 547 F. Supp. 2d at 996-97 (sharing

[REDACTED]

the concerns expressed in Mayfield that the significant purpose test violates the Fourth Amendment, but not reaching the issue because of finding that the primary purpose of the surveillance in that case was to gather foreign intelligence and not to prosecute the defendant for criminal activity).

[REDACTED] This Court disagrees with the holding of the Mayfield court and finds that FISA's "significant purpose" test is consistent with the Fourth Amendment's requirement of reasonableness. Moreover, the Court agrees with the discussion of the FISC of Review regarding the differences between law enforcement in ordinary investigation and law enforcement in the national security context. Defendants additionally argue that additional aspects of FISA render it in violation of the Constitution. These arguments will be discussed in turn.

[REDACTED] First, Defendants argue FISA is unconstitutional because it lacks a requirement that the government show that a crime has been or is being committed. The probable cause requirement under FISA is different than the probable cause to seek a Title III wiretap. As noted by Judge Easterbrook in United States v. Ning Wen, 477 F.3d 896 (7th Cir. 2007), however, "the probable cause of which the fourth amendment speaks is not necessarily probable cause to believe that any law is being violated." *Id.* at 898. The court in that case analogized the probable cause required by FISA to the probable cause requirements for administrative search warrants, which may issue on probable cause to believe that the government has adopted a reasonable system of regulations and inspections and is not targeting individuals for improper reasons. The Supreme Court in Keith recognized that Congress is constitutionally permitted to set different standards for probable cause in the context of foreign intelligence surveillance than in ordinary criminal surveillance. This different probable cause requirement does not render FISA in

[REDACTED]

violation of the Fourth Amendment.

[REDACTED] Defendants also contend that FISA impermissibly allows the government to satisfy the FISA application requirements without explaining to the FISA Court how they are met. This argument is incorrect; the FISA Court and later the district court in a criminal prosecution must find that the statutory requirements were met after *ex parte*, in camera review of the government's application. Neither court simply accepts the government's certification that the requirements are met without evaluating whether probable cause, as defined by the FISA, exists, and whether the other statutory requirements, as detailed above, have been met.

[REDACTED] Next, Defendants argue the "clearly erroneous" standard of review allows the government to avoid traditional judicial oversight. Even in the context of a warrant issued under Title III, statements made in a warrant application are given deference and evaluated under the *Franks* standard. See *Franks* discussion, *supra*. The Court has already applied the *Franks* standard to the statements underlying the FISA applications in this case.

[REDACTED] In addition, Defendants argue the government may retain and use FISA-derived information without providing a defendant with a meaningful opportunity to challenge a FISA order. This is a challenge to the *ex parte*, in camera review contemplated by FISA. Defendants seek disclosure of the currently classified applications so that they may more effectively challenge the FISA orders. As noted above, while other courts have sympathized with the difficulty of Defendants' position and the uphill battle they face in challenging orders of which they cannot know the content, such a system is permissible given the requirements of foreign intelligence gathering. See, e.g., *Mubayyid*, 521 F. Supp. 2d at 131.

[REDACTED] Defendants argue further that without a criminal prosecution, no notice is ever given

[REDACTED]

to a target that FISA-approved surveillance has occurred, and the notice provisions in general are impermissibly broad. The government argues, and the Court agrees, that Defendants do not have standing to raise this issue because a criminal prosecution was initiated in this case and the Defendants were given notice.

[REDACTED] Moreover, Defendants maintain FISA violates the Fourth Amendment because no showing of particularity is required, resulting in an impermissible general warrant. This argument is linked to Defendants' argument that the probable cause requirements of the FISA are impermissibly less than the probable cause requirements of a Title III warrant. Because the Court finds that FISA's lesser probable cause standard is constitutional, the resulting order cannot be classified as an impermissible general warrant.

[REDACTED] Likewise, Defendants argue FISA is unlawful in that the allowance of 120 days of surveillance for U.S. persons violates the durational limits for Title III warrants in criminal investigations. Although the duration of surveillance pursuant to a FISA warrant is longer than surveillance pursuant to a Title III warrant, this is reasonable because of the nature of national security surveillance, which is often long range and involves the interrelation of various sources. See *Kerth*, 407 U.S. at 322.

[REDACTED] Finally, the government argues that even if the Court determines that FISA is unconstitutional, the evidence obtained pursuant to the FISA orders in this case should still be admissible because the government relied on the constitutionality of FISA and the FISA orders in good faith. Because *Mayfield* was a facial challenge to the constitutionality of FISA in the context of a civil suit against the government, the court in that case did not have occasion to comment on issues related to suppression of evidence. Because the Court concludes that FISA is

[REDACTED]

constitutional, an inquiry into whether the agents in this case acted in good faith is not required. Mubayyid, 521 F. Supp. 2d at 140 n.12 ("Even if the statute were deemed unconstitutional, there appears to be no issue as to whether the government proceeded in good faith and in reasonable reliance on the FISA orders. The exclusionary rule would thus not appear to apply under the rule of United States v. Leon, 468 U.S. 897 (1984).")

In sum, the Court rejects Defendants' constitutional challenges to FISA. At its heart, the Fourth Amendment requires that searches and seizures be reasonable, and though the procedure for obtaining a FISA order and for judicial review of that order does differ from a obtaining a warrant under Title III and for judicial review of that warrant, those procedures are reasonable, particularly given the decisions of Congress and the Supreme Court that the context of foreign intelligence surveillance is different than ordinary law enforcement surveillance. The Court concludes that the FISA, as amended by the Patriot Act, is constitutional.

V. [REDACTED] MISCELLANEOUS NONMERITORIOUS ARGUMENTS

A. [REDACTED] Alleged Violation of § 1806(f)'s Notice Requirement

Eljvir Duka argues the government violated 50 U.S.C. § 1806(f) by using FISA-obtained evidence prior to giving notice to the Court. Specifically, he guesses that the government used FISA-obtained evidence in the grand jury proceedings for this case and when obtaining search warrants. Eljvir Duka argues further that prior to any such use the government must obtain from the Court a determination that the FISA evidence sought to be used was obtained lawfully. The government states it did not use any FISA-obtained evidence in the grand jury proceedings or when obtaining search warrants. Accordingly, Eljvir Duka's argument on this point is not relevant.

[REDACTED]

B. [REDACTED] Attorney General's Authorization Required by § 1806(b)

[REDACTED] Eljvir contends the Government has not revealed written authorization of the Attorney General to use FISA evidence in this case in accordance with § 1806(b). "No information acquired pursuant to this subchapter shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General." 50 U.S.C. § 1806(b).

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

C. [REDACTED] Attorney General's Affidavit Pursuant to 50 U.S.C. § 1806(f)

Eljvir argues the government has not filed an affidavit by the Attorney General that the FISA materials used in the past or sought to be used in the future are a matter of national security or otherwise classified by statute pursuant to § 1806(f). The government submitted this affidavit with its filings in opposition to Defendants' motions, however; therefore, this issue is moot.

Dated: 8-14-08

Robert B. Kugler
ROBERT B. KUGLER
United States District Judge